Clarity, Courage, and Action

Presented to: California Privacy Steering Team
By Laura Landry, Executive Director, laura.landry@whinit.org, 562-436-2923 x 222

Goals

- Reducing provider provider FEAR of data exchange
- Set the Stage for ACTIONABLE privacy and security discussions in California and the U.S.
- Build MOMENTUM and CONSENSUS for forward movement
- Recruit participants to build out the rational ROADMAP and model(s)

Definitions

- ***Context***

1. The circumstances that form the setting for an event, statement, or idea, and in terms of which it can be fully understood and assessed.
2. The parts of something written or spoken that immediately precede and follow a word or passage and clarify its meaning.

- ***Privacy***

1a : the quality or state of being apart from company or observation : seclusion b : freedom from unauthorized intrusion <one's right to privacy>

2archaic : a place of seclusion

3a : secrecy b : a private matter : secret

- ***Confidentiality***

1: marked by intimacy or willingness to confide <a *confidential* tone>

2: private, secret <*confidential* information>

3: entrusted with confidences <a *confidential* clerk>

4: containing information whose unauthorized disclosure could be prejudicial to the national interest — compare secret, top secret

- ***Information security***

1: protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.

Terms as Used in Privacy Discussions

- Data – bits and bytes, the elemental components of electronic storage
- "Information "– bits with meaning
- It is allowable to protect "information" via encryption, even when the containing of the "data" is accessible.
- "Confidential" is generally is used to refer to a quality of information (that needs to be protected),
- "Privacy" refers to a quality or state of an individual.
- Information security is defined (including HIPAA) as the protection of the confidentiality of sensitive information, the integrity of data, and the availability of services and resources.

The Conundrum

- Privacy and Security
  - A California citizen has a "right to privacy" state
    - You can, however, waive it (Smartphone location services, anyone?)
- The nation is in an uproar around consumer privacy
  - The uproar is not the issue
  - The issue is that organizations have benefitted from a patient's information and potentially caused harm to the patient 's ability to receive insurance or other issues
  - The disconnect is that the average person assumes that the people giving them care have what they need to do their jobs
- Healthcare is perceived to have played fast and loose with patient information
  - Sometimes selling patient data for profit
  - Sometimes making mistakes with the best of intentions

The Furor

- It's a NUMBERS game
  - If someone loses a paper chart
    - It's one person's data
  - If someone loses a disc of data or is hacked
    - It's data in the thousands
  - And that large volumes of data can be sent throughout the world within seconds and with a low probability of being detected – or used to steal identities or commit fraud
- Do organizations need to be diligent? Yes!
- Is the ability to delivery healthcare currently paralyzed due to fear and confusion? Yes!

Higher Standard for Electronic Data

- A fax machine does not provide access to "thousands of records with identity information"
  - The perception is that current paper breaches are one at a time, or at worst hundreds at a time
  - The reality -- Fax servers are capable of causing large scale breaches, as well
- Banks manage to keep private records private
  - Healthcare delivery resources have varying levels of expertise
  - It is an unfunded mandate –
    - ATMs collect fees
    - Providers don't (yet) add a "security fee" to your medical bill
- Control of medical records = Control of online banking
  - Maybe one day…

Expectations of Privacy -- Demystified

Context	Financial Responsibility	Privacy Expectation	Expectation of Confidentiality
Emergency Room	Health Plan	Low	High
Encounter	Health Plan	Moderate	High
Encounter	Patient	High	High
Encounter	No Pay/Charity	Low	High

This table can generally be summed up:
A person expects their information to be shared with their insurance company for payment, the labs to do tests, the physicians who ordered the tests, the nurses who support the doctors, and pharmacies. But not with other entities who have no role associated with their encounter.

Note: The above is solely starting point, as a way of looking at the issues to set up the appropriate discussions geared toward creating solutions and/or clarity.

Privacy FROM Whom?

- Physicians? No
- Care team? No
- Employers? Yes
- Payers? Yes (if I pay cash); No (if Payer pays)
- What are the costs and trade-offs of absolute privacy?
  - Unsustainable costs
  - Unaffordable health insurance
  - Medical errors
  - And (ultimately) avoidable loss of life
- Do my privacy requirements change from time to time?
  - Yes

So what are we all afraid of?

- Lawsuits
  - Deep pockets pay high fines
- No industry agreement on what works
  - Or even what needs protecting
- Nobody knows what "Enough" protection is

Contributing to the Problems…

- Most EHR solutions do not handle consent at all
- The duty to educate the patient resides somewhere – and in an already over-regulated industry, whose job is it?
  - ONC Privacy Tiger Team says it's the caregiver
- Patient identification across organizations is the #1 problem
  - Relies on insurance (annual policy turnover 20%-30%)
  - Large populations have high incidence of "common names"

So what's the Roadmap?

- Create Transparency
  - Why do people exchange data and for what purposes
    - Consumers should not be "surprised" by an exchange of data
  - Auditability – it is essential to proactively review access activity so that we police ourselves and trust can be re-established with patients
- Re-establish Precision of Language
  - The industry must agree to the scenarios, and use the right terms to describe the access to data
  - Impermissible uses must be clearly spelled out
- Work together to develop privacy-related metadata so that rules can be used to govern access in different circumstances
- Work with advocacy agencies/groups to update existing laws and regulation for the 21st Century healthcare delivery system

Apply a Standared like The Reasonable Person (source: Wikipedia)

- The **reasonable person** (historically *reasonable man*) is a legal fiction of the common law representing an objective standard against which any individual's conduct can be measured. It is used to determine if a breach of the standard of care has occurred, provided a duty of care can be proven.
- The reasonable person standard holds: each person owes a duty to behave as a reasonable person would under the same or similar circumstances. While the specific circumstances of each case will require varying kinds of conduct and degrees of care, the reasonable person standard undergoes no variation itself.
- This standard performs a crucial role in determining negligence in both criminal law—that is, criminal negligence—and tort law. The standard also has a presence in contract law, though its use there is substantially different.
- The standard does not exist independently of other circumstances within a case which could affect an individual's judgment.

Framework for moving forward

- Define the need for the transfer and use of information in scenario based way that everyone can easily understand
  - A new patient in a physician's office – does the physician need to get the patient's consent to see previous records? Yes
  - An existing patient in a physicians office who was sent to a referring physician, does the doctor need to get the patient's consent? No
- Define what is absolutely not allowable
  - Selling identified data
  - Selling insufficiently de-identified data that can be re-identified
  - Etc.

CURRENT PROCESS –
Get a signed consent at each site/organization to access patient data

Patient Arrives
At hospital

NOTE: This is probably the same
As any site, but we were
Talking about a hospital at the time we
Created this workflow

Compos mentis –
1) NOPP – paragraph re:participation in WHIN
2) Patient Authorization (patient gets copy)

Non compos mentis ***or*** that it is a defined medical emergency–
• Break the glass

Patient gives consent --
Clinician makes an assertion of
Having the signed authorization form
And accesses the data

Clinician makes an assertion of
Medical emergency, and accesses
The data

Patient denies consent –
Either set it in the portal ("No") or hospital can fax or secureeMail a form to have WHIN do it.

Operational Considerations --

a) Educate registration/intake staff on what WHIN is and what we do
b) Add the patient authorization form to the training for registration/intake staff
c) Can hospital registration system set a "consent authorization received" checkbox from its registration screen? This should be specific to the patient, not the encounter, so should be stored in the medical record. Alternatively, could get authorization for each event (might be easier process, but more convoluted paperwork over time)

Pre-Authorization –
e.g. Scheduled surgery, MRI, Labor & Delivery, etc.

Physician/Surgeon Office would gather the consent for themselves

Can the physician office authorize the hospital to view patient data based on the established "treatment relationship"

Current process:
(Patient is not included in the current process.)
Surgeon's office calls for availability to the O.R. scheduling desk
Patient gets on the hospital's surgical schedule
O.R. paperwork people work with the surgeon's office to get information on the patient.
Surgeon's office faxes labwork and other important information to O.R. or O.R. gets information directly from lab
-- this is a well-defined business to business treatment related relationship --

Chain of trust assumption – that the primary care physician has a relationship with the surgeon, the surgeon/hospital doesn't have a relationship with other sources, and the data from other sources will be either not Reviewed or only reviewed because it was deemed "necessary" to the current episode. This is the same assumption that allows the "Continuity of Care Document" to be shared – because there is no "minimum necessary" in developing a CCD. Audit logs for O.R. patients can be made available for periodic review.

"Speed Solution-ing" Workshop

- What are the top 10 scenarios to move data?
  - Make your OWN list on a piece of paper now
- What are the 10 most mis-used terms in the Privacy and Security conversations?
  - Make your OWN list on a piece of paper now
- What are 3 actions you can take to create clarity?
- PLEASE make a copy of your lists, and provide them to the CalOHII staff before you leave
  - We will collate these lists, and start working from them to drive statewide solutions